LAB 2 Single-Segment IP Networks **Part 1.**

Name:

Using Filters in Tcpdump

Exercise 1: Writing Filter Expressions for Tcpdump

Step 1.

- Question: Give the tcpdump command:
  - **Answer:**
- Include the saved data in your lab report.

Step 3.

- Question: Give the tcpdump command:
  - **Answer:**
- Include the saved data in your lab report.

Part 2. Using Filters in Wireshark

Exercise 2(A):

- **Revision : Use the option „print summary“**

Exercise 2(B): Working with Display Filters:

Step 3.

- Question: Give the display command:
- **Answer:**

Step 4.

- Include the saved data in your lab report.

Step 5.

- Question: Give the display command
- **Answer:**

- Include the saved data in your lab report.

Exercise 2(C): More Complex Capture and Display Filters

Step 5a.

- Question: Give the display command
  - **Answer:**

- Include the saved data in your lab report.

Step 5b.

- Question: Give the display command
  - **Answer:**

- Include the saved data in your lab report.

Step 5c.

- **Revision : use destination port = 23**
- Question: Give the display command
  - **Answer:**

- Include the saved data in your lab report.

Part 3. ARP – Address Resolution Protocol

Exercise 3(A): A Simple Experiment with ARP

Step 5

- Include the saved data in your lab report.

Lab Report

- Question: What is the destination MAC address of an ARP Request packet?
  - **Answer:**

- Question: What are the different values of the Type field in the Ethernet headers that you observed?
  - **Answer:**

- Question: Use the captured data to discuss the process in which ARP acquires the MAC address for IP address 10.0.1.12.
  - **Answer:**

Exercise 3(B): Matching IP Addresses and MAC Addresses

Lab Report:

- Question: Include the completed Table 2.2 in your lab report.

Linux PC	IP Address of Ethernet Interface eth0	MAC Address of Ethernet Interface eth0
PC1	10.0.1.11/24	
PC2	10.0.1.12/24	
PC3	10.0.1.13/24	
PC4	10.0.1.14/24	

Exercise 3(C): ARP Requests for a Nonexisting Address

Step 3

- Include the saved data in your lab report.

Lab Report

- Question: Using the saved output, describe the time interval between each ARP Request issued by PC1.
  - **Answer:**

- Question: Describe the method used by ARP to determine the time between retransmissions of an unsuccessful ARP Request. Include relevant data to support your

answer.

- **Answer:**

- Question: Why are ARP Request packets not transmitted (i.e., not encapsulated) like IP packets? Explain your answer.
  - **Answer:**

Part 4. The Netstat Command

Exercise 4

Step 1.

- Include the saved data in your lab report.

Step 2.

- Include the saved data in your lab report.

Step 3.

- Include the saved data in your lab report.

Step 4.

- Include the saved data in your lab report.

Lab Report

- Question: What are the network interfaces of PC1 and what are the MTU (maximum transmission unit) values of the interfaces?
  - **Answer:**

- Question: How many IP datagram, ICMP messages, UDP datagram, and TCP segments has PC1 transmitted and received since it was last rebooted?
  - **Answer:**

- Question: Explain the role of interface lo, the loopback interface. In the output of netstat –in, what are the values of RX-OK (packets received) and TX-OK (packets transmitted) different for interface eth0 but identical for interface lo?
  - **Answer:**

Part 5. Configuration IP Interfaces in Linux

Exercise 5: Changing the IP Address of an Interface

Step 1.

- Include the saved data in your lab report.

Step 3.

- Include the saved data in your lab report.

Lab Report

- Question: Explain the fields of the ifconfig output.
  - **Answer:**

Part 6. Duplicate IP Addresses

Exercise 6

Step 6.

- Include the first captured TCP and ARP packets in your lab report (show the MAC address of each frame)

- Include the saved ARP cache in your lab report.

Lab Report

- Question: Explain why the Telnet session was established to one of the hosts with the duplicate address and not the other. Explain why the Telnet session was established at all and did not result in an error message. Use the ARP cache and the captured packets to support your explanation.
  - **Answer:**

Part 7. Changing Netmasks

Exercise 7

Step 2a.

- Include the captured data in your lab report.

- Include the output of the ping command in your lab report.

- Question: Use your output data and ping results to explain what happened in each of the ping commands. Was the ping operations successfully ?
  - **Answer:**

Step 2b.

- Include the captured data in your lab report.

- Include the output of the ping command in your lab report.

- Question: Use your output data and ping results to explain what happened in each of the ping commands. Was the ping operations successfully ?
  - **Answer:**

Step 2c.

- Include the captured data in your lab report.

- Include the output of the ping command in your lab report.

- Question: Use your output data and ping results to explain what happened in each

of the ping commands. Was the ping operations successfully ?

- **Answer:**

Step 2d.

- Include the output of the ping command in your lab report.

- Question: Use your output data and ping results to explain what happened in each of the ping commands. Was the ping operations successfully ?
  - **Answer:**

Step 2e.

- Include the output of the ping command in your lab report.

- Question: Use your output data and ping results to explain what happened in each of the ping commands. Was the ping operations successfully ?
  - **Answer:**

Step 2f.

- Include the output of the ping command in your lab report.

- Question: Use your output data and ping results to explain what happened in each

of the ping commands. Was the ping operations successfully ?

- **Answer:**

Part 8. Static Mapping of IP Addresses And Host Names

Exercise 8: Associating Names with IP Addresses

Lab Report

- Question: Explain why a static mapping of names and IP addresses is impractical when the number of hosts is large.
  - **Answer:**

- Question: What will be the result of the host name resolution when multiple IP addresses are associated with the same host name in the /etc/hosts file?
  - **Answer:**

Part 9. Experiments with FTP and Telnet

Exercise 9(A): Snoop Passwords from an FTP session

- **Revision: use the option “display-filter” and ”print as displayed”**

Step 5.

- Include the saved data in your lab report.

Lab Report

- Question: Using the saved output, identify the port numbers of the FTP client and the FTP server.
  - **Answer:**

- Question: Identify the login name and the password, shown in plain text in the payload of the packets that you captured.
  - **Answer:**

Exercise 9(B): Snoop Passwords from a Telnet session

- Include the saved data in your lab report.

Lab Report

- Question: Does Telnet have the same security flaws as FTP? Support your answer using the saved output.
  - **Answer:**

Exercise 9(C): Observe traffic from a Telnet session

Step 4.

- Include the saved data in your lab report.

Lab Report

- Question: Explain why three packets are sent in a Telnet session for each character typed on the terminal.
  - **Answer:**